

Image Hiding by Square Fully Exploiting Modification Directions

Wen-Chung Kuo

Department of Computer Science and Information Engineering
National Yunlin University of Science & Technology
123 University Road, Section 3, Douliou, Yunlin 64002
simonkuo@yuntech.edu.tw

Received February, 2013; revised February, 2013

ABSTRACT. *In order to quick embedding secret and improve the data hiding capacity from 1 bpp to 4.5 bpp, a new data hiding scheme by square fully exploiting modification directions method will be proposed in this paper. According to experiment results, we can prove that proposed scheme not only to enhance the embedding rate and good embedding capacity but also to keep stego-image quality.*

Keywords: Data hiding, Extracting function, Stego-image, Modulus operation.

1. **Introduction.** Due to the rapid growth of network and smart phone technology, a lot of private image information such as digital photos or videos communicates in Internet. Thus, people can be shared the happy or unhappy things each other, immediately. However, there are many attacks such as illegal duplication, forgery and spoofing when digital multimedia is transmitted through this public channel. Therefore, how to protect the digital data security has become very important. A smart way to solve this problem is to hide personal data behind a meaningful image such that an unintended observer will not be aware of the existence of the hidden secret message. Until now, many data hiding schemes based on different methods (such as direct or undirect) have been proposed[1, 2, 3, 4, 5, 6, 7, 10]. From the direct view, the most common data hiding technique is the least significant bit replacement method (LSB-R) proposed. Its major embedding formula is that the secret data will be embedded into the k th bit ($1 \leq k \leq 8$) of each pixel of the cover image. The stegoimage quality for LSB-R is acceptable, since it has been determined that human perception cannot detect the secret data embedded in the cover image when $k \leq 3$ (i.e. the 3 least significant bits). From the undirect view, i.e. using the embedding function, a data hiding scheme based on the Exploiting Modification Direction (EMD) method to achieve the data hiding goal is proposed by Zhang and Wang [10] in 2006. The EMD-scheme characteristically uses the relationship of n adjacent pixels to embed the secret data. That is to say, the binary secret data stream will be separated into blocks and transformed into a $(2n + 1)$ -ary. Then, this secret will be embedded into n adjacent pixels where $n > 1$. For instance, if the secret data is embedded in two adjacent pixels, i.e., it only modifies only one of two adjacent pixels in the EMD scheme - add one, subtract one, or stay the same. From the experimental results, they claimed that EMD-scheme can enhance secret data embedding capacity and maintain good stego-image quality. Since then, in order to improve the embedding capacity, there are many EMD-type steganographic methods have been proposed [3, 4, 5]. 2007, Lee et al.[5] proposed

an improvement scheme (HC-EMD) in order to enhance the embedding ratio from 1 bpp to 1.5 bpp. Recently, Kuo and Wang proposed a GEMD (general exploiting modification direction) data hiding scheme[3] to improve the embedding capacity notation from $(2n + 1)$ to (2^{n+1}) -ary. Basically, the HC-EMD scheme proposed by Lee et al.[4] that the parameter n is limited to 2 is also the special case of Kuo-Wang scheme. Laterly, Kieu and Chang[2] provided a new embedding function called fully exploiting modification direction (FEMD) and then a robust data hiding scheme based on the FEMD method is proposed to improve the original data hiding capacity from 1 bpp to 4.5 bpp. According to the Kieu-Chang scheme, they use this new function with the search matrix to embed the secret data. In order to quick embedding secret data, a new data hiding scheme based on square fully exploiting modification directions method will be proposed in this paper. In fact, we will propose a new extraction function and then provide a formula to finish the shifting direct and distance when the secret data is embedded. Finally, our experiment results prove the proposed scheme not only enhances the embedding rate and good embedding capacity but also keeps stegoimage quality. This paper is organized as follows: Section 2 will introduce the EMD-scheme and Kieu-Chang scheme. Then, we will propose a new data hiding scheme based on square fully exploiting modification direction in Section 3 and give the experimental results in Section 4. Finally, concluding remarks will be given in Section 5.

2. Review two data hiding schemes. Until now, many data hiding techniques have the problem of balancing image distortion and data hiding capacity. In order to solve this problem, Zhang and Wang had been proposed the EMD data hiding scheme which can provide higher data capacity and higher PSNR (above 50dB). In this section, we will review Zhang-Wang scheme[10] and Kieu-Chang scheme[2] in detail.

2.1. Data Hiding Scheme based on EMD. In 2006, Zhang and Wang proposed a novel data hiding scheme based on the exploiting modification direction method[10]. The characteristic of the EMD scheme is that propose a weighing extraction function to embed secret data into a cover image. Therefore, Zhang and Wang propose the following extraction function shown as Eq.(1):

$$f(x_1, x_2, \dots, x_n) = \sum_{i=1}^n x_i \times i \quad \text{mod } (2n + 1) \quad (1)$$

where x_i is the i^{th} pixel value, n as the number of pixels. For example, the 5-ary secret data stream will be embedded in two adjacent pixels, i.e., it only modifies one of two adjacent pixels in the EMD scheme - add one, subtract one, or stay the same. Here, some notations are defined for introducing the EMD-scheme.

I_C : The grayscale cover image.

$O_{EMD}()$: Obtain all n -tuples $(x_1, x_2, \dots, x_n)$ from partitioning the image I_C into the non-overlapping n -pixel blocks by scanning from the left side to right side and from top to down, as shown in Fig. 1.

$O_{EMD-S}()$: Obtain $(2n + 1)$ -ary data m from partitioning the binary secret data stream M for each block.

Algorithm EMD (Embedding Algorithm for EMD Scheme):

Input: The cover image I_C and binary secret data stream M .

Output: The stegoimage I_S .

(EMD-1): Obtain all n -pixel blocks $(x_1, x_2, \dots, x_n)$ from I_C and $O_{EMD}(I_C)$ and the secret data m_1 from $O_{EMD-S}(M)$;

(EMD-2): For each block, calculate $t = f(x_1, x_2, \dots, x_n)$;

(EMD-4): If $(d = 0)$, then $(y_1, y_2, \dots, y_n) = (x_1, x_2, \dots, x_n)$,

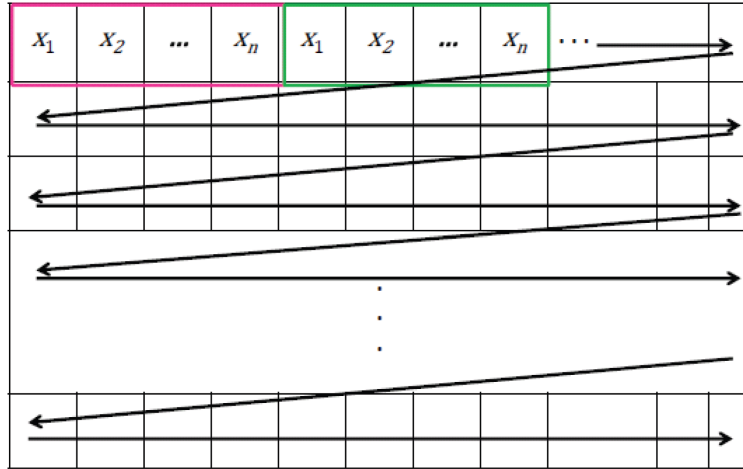


FIGURE 1. The embedding data sequence for EMD

(EMD-5): Modify the $(x_1, x_2, \dots, x_n)$ in I_C by $(y_1, y_2, \dots, y_n)$ to create I_S .

Example 2.1. Let adjacent five pixels $(x_1, x_2, x_3, x_4, x_5) = (131, 128, 130, 129, 129)$ and secret data $m_1 = (1001)_2$. Using the EMD scheme and following steps, we find the five stego pixels $(y_1; y_2, y_3, y_4, y_5) = (130, 128, 130, 128, 129)$.

(Step4) :Get the stego pixels $(y_1, y_2, y_3, y_4, y_5) = (131, 128, 130, 128, 129)$.

$$F(x_i, x_{i+1}) = [x_i \times (s-1) + x_{i+1} \times s] \mod s^2 \quad (2)$$

Subsequently, Kieu and Chang use the search matrix structure $W_{(2r+1) \times (2r+1)}(s, (x_i, x_{i+1}), r)$ to embed the secret data. In other words, the k-bit secret data can be embedded into

	0	1	2	3	4	5	6	7	...	255	x_{i+l}
0	0	3	6	0	3	6	0	3	...	0	
1	2	5	8	2	5	8	2	5	...	2	
2	4	7	1	4	7	1	4	7	...	4	
3	6	0	3	6	0	3	6	0	...	6	
4	8	2	5	8	2	5	8	2	...	8	
5	1	4	7	1	4	7	1	4	...	1	
6	3	6	0	3	6	0	3	6	...	3	
7	5	8	2	5	8	2	5	8	...	5	
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	...	$\vdots$	
255	6	0	3	6	0	3	6	0	...	6	

x_i ↓

FIGURE 2. S -matrix when modulus $s = 3$

pair (x_i, x_{i+1}) of cover image by using the S -matrix structure with the search range r , where $k = \log_2 s^2$ and $r = s/2$. For example, given the pair pixel $(x_i, x_{i+1}) = (4, 3)$ and $s = 4$, the resultant search matrix $W_{5 \times 5}(4, (4, 3), 2)$ is shown as Fig.3. In order to reduce stego-image distortion, Kieu and Chang use the minimum distortion strategy method shown as Eq.(3) to select local optimal solution $D_{\min}$ in $S[x_j][y_j]$.

$$D_{\min} = \min_{j=a,b,c} \{|x_i - x_j| + |x_{i+1} - y_j|\} \quad (3)$$

Now, we give an example to explain the Kieu-Chang scheme as following.

	0	1	2	3	4	5	6	7	8	9	...	x_{i+l}
0	0	4	8	12	0	4	8	12	0	4	...	
1	3	7	11	15	3	7	11	15	3	7	...	
2	6	10	14	2	6	10	14	2	6	10	...	
3	9	13	1	5	9	13	1	5	9	13	...	
4	12	0	4	8	12	0	4	8	12	0	...	
5	15	3	7	11	15	3	7	11	15	3	...	
6	2	6	10	14	2	6	10	14	2	6	...	
7	5	9	13	1	5	9	13	1	5	9	...	
8	8	12	0	4	8	12	0	4	8	12	...	
9	11	15	3	7	11	15	3	7	11	15	...	
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	...	

x_i ↓

FIGURE 3. The search matrix $W_{5 \times 5}(4, (4, 3), 2)$ when $s = 4$

Example 2.2. Let adjacent two pixels $(x_i, x_{i+1}) = (4, 3)$ and $s = 4$ and secret data $m_2 = 6$. According to Fig.3, we can find three possible locations as $S[2][4]$, $S[6][1]$ and

$S[6][5]$ in the range of search matrix $W_{5 \times 5}(4, (4, 3), 2)$. Then, using the Eq.(3), we can find out the local optimal solution is $(y_i, y_{i+1}) = (2, 4)$.

However, by using the FEMD data hiding method, it must need a storage place to store the search matrix and then they use the match method when the secret data is embedded. As a result, it is time-consuming and impractical for this method.

3. Propose a data hiding scheme based on square FEMD. In order to enhance the embedding rate and provide a close solution form to the extraction function shown as Eq.(4), a new data hiding scheme based on square fully exploiting modification directions (so call SFEMD) is proposed in this section. Furthermore, to enhance information security, we can use existing encryption technology (such as DES or AES) to encode the secret message before the embedding procedure. Now, we propose a new extraction function $F_s(x_i, x_{i+1})$ as following:

$$F_s(x_i, x_{i+1}) = [x_i \times (s^2 - 1) + x_{i+1} \times s^2] \mod s^4 \quad (4)$$

where x_i is the i_{th} pixel value, s is the weighting coecient. In order to solve (x_i, x_{i+1}) quickly, we will propose a theorem to satisfy this requirement.

Theorem 3.1. If $F_s(x_1, x_2)$ and modulus s are given, then we can find out (x_1, x_2) directly, $x_1 = (s^2 - 1) \times F_s(x_1, x_2) \mod s^2$ and $x_2 = (\frac{(F_s(x_1, x_2) - (s^2 - 1 \times x_1))}{s^2}) \mod s^2$, such that $F_s(x_1, x_2) = [x_1 \times (s^2 - 1) + x_2 \times s^2] \mod s^4$.

In order to understand the theorem 3.1, we give an example to explain it.

Example 3.1. If $F_s(x_1, x_2) = 10$ and $s = 2$, then the pair $(x_1, x_2) = (2, 1)$ by the following steps.

(Step 1): From $s = 2$, we can get $F_s(x_1, x_2) = x_1 \times 3 + x_2 \times 4 \mod 16$.

(Step 2): Compute $x_1 = 3 \times 10 \mod 4 = 2$.

(Step 3): Calculate $x_2 = (\frac{(10 - 3 \times 2)}{4}) \mod 4 = 1$.

3.1. Embedding Procedure. So, there are some notations are defined before we introduce the SFEMD scheme.

$O_{SFEMD}()$: Obtain all 2-tuples (x_1, x_2) from partitioning the image IC into the non-overlapping 2-pixel blocks by scanning from the left side to right side and from top to down, as shown in Fig. 4.

$O_{SFEMD-S}()$: Obtain s^4 -ary data m from partitioning the secret data stream M for each block.

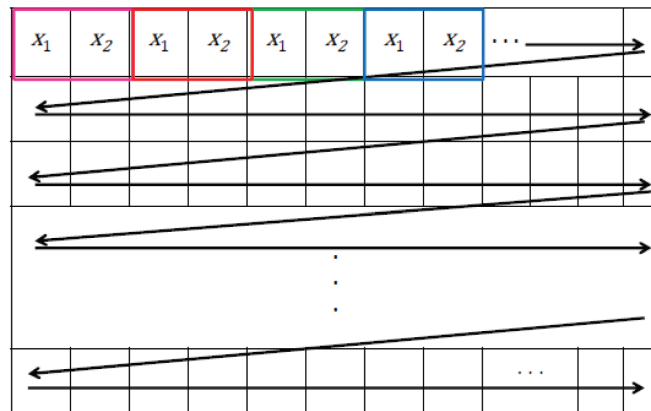


FIGURE 4. The embedding data sequence for SFEMD scheme

Embedding Algorithm:**Input:** Cover image I_C and the secret data stream M .**Output:** Stego-image I_S .(SFEMD-1): Obtain all 2-pixel blocks (x_1, x_2) from I_C and $O_{SFEMD}(I_C)$;(SFEMD-2): Obtain m_1 from $O_{SFEMD-S}(M)$ for each block;(SFEMD-3): Calculate $d = F_s(x_1, x_2) = [x_1 \times (s^2 - 1) + x_2 \times s^2] \bmod s^4$;(SFEMD-4): If $d = m_1$ then $(x_1, x_2) = (y_1, y_2)$; Otherwise, compute

$$1. t = (s^2 - 1) \times m_1 \bmod s^2;$$

$$2. t_{1,1} = t - (x_1 \bmod s^2);$$

$$3. \text{ If } t_{1,1} > 0, \text{ then } t_{1,1} = t_{1,1} - s^2;$$

$$4. y_{1,1} = y_{2,1} = x_1 + t_{1,1};$$

$$5. \text{ Compute } t_{1,2} = \left[\frac{(m_1 - (s^2 - 1)) \times y_{1,1}}{s^2} \right] \bmod s^2;$$

$$6. \text{ Compute } t_{1,2} = t_{1,2} - (x_2 \bmod s^2) \text{ and if } t_{1,2} > 0, \text{ then } t_{2,2} = t_{1,2} - s^2, \text{ else } t_{2,2} = t_{1,2} + s^2;$$

$$7. \text{ Compute } y_{1,2} = x_2 + t_{1,2} \text{ and } y_{2,2} = x_2 + t_{2,2};$$

$$8. \text{ Compute } t_{2,1} = t_{1,1} + s^2;$$

$$9. \text{ Compute } y_{3,1} = y_{4,1} = x_1 + t_{2,1};$$

$$10. \text{ Compute } t_{3,2} = \left[\frac{(m_1 - (s^2 - 1)) y_{2,1}}{s^2} \right] \bmod s^2;$$

$$11. \text{ Compute } t_{3,2} = t_{3,2} - (x_2 \bmod s^2) \text{ and if } t_{3,2} > 0, \text{ then } t_{4,2} = t_{3,2} - s^2, \text{ else } t_{4,2} = t_{3,2} + s^2;$$

$$12. \text{ Compute } y_{3,2} = x_2 + t_{3,2} \text{ and } y_{4,2} = x_2 + t_{4,2};$$

(SFEMD-5): Compute distortions from $D = \{(|x_1 - x| + |x_2 - y|) | (x, y) \in \{(y_{1,1}, y_{1,2}), (y_{2,1}, y_{2,2}), (y_{3,1}, y_{3,2}), (y_{4,1}, y_{4,2})\}\}$ (SFEMD-6): Select a (x, y) with minimum distortion in D , and let stego pixel pair $(y_1, y_2) = (x, y)$.

Here, we give an example to explain the embedding algorithm.

Example 3.2. If the pixels pair is $(x_1, x_2) = (163, 167)$ and the secret data $m_3 = 13$ when $s = 4$, then the stego-image's pixels pair $(y_1, y_2) = (163, 168)$ by the following steps.(Step 1): Calculate $d = [163 \times 15 + 16 \times 167] \bmod 256 = 61 \neq 13$;

(Step 2): Compute

$$1. t = 15 \times 13 \bmod 16 = 3;$$

$$2. t_{1,1} = 3 - (163 \bmod 16) = 0;$$

$$3. y_{1,1} = y_{2,1} = x_1 + t_{1,1} = 163;$$

$$4. t_{1,2} = \left(\frac{13 - 15 \times 163}{16} \right) \bmod 16 = 8;$$

$$5. t_{1,2} = 8 - (167 \bmod 16) = 1 \text{ and } t_{2,2} = 1 - 16 = -15;$$

$$6. y_{1,2} = 167 + 1 = 168 \text{ and } y_{2,2} = 167 - 15 = 152;$$

7. $t_{2,1} = t_{1,1} + s^2 = 0 + 16 = 16$;
8. $y_{3,1} = y_{4,1} = 163 + 16 = 179$;
9. $t_{3,2} = (\frac{13-15 \times 179}{16}) \bmod 16 = 9$;
10. $t_{3,2} = 9 - (167 \bmod 16) = 2$ and $t_{4,2} = 2 - 16 = -14$;
11. $y_{3,2} = 167 + 2 = 169$ and $y_{4,2} = 167 - 14 = 153$;

(Step 3): Compute all distortions from $\{(163, 168), (163, 152), (179, 169), (179, 153)\}$.
 (Step 4): Select $(163, 168)$ with minimum distortion as the stego pixel pair.

3.2. Extraction Procedure. The designated receiver can recover the secret data when receiving stego-image I_S . The extraction algorithm is detailed as following:

Extraction Algorithm:

Input: Stegoimage I_S .

Output: The binary secret data stream M .

(ESFEMD-1): Obtain all 2-pixel blocks (x_1, x_2) from I_S and $O_{SFEMD}(I_S)$.

(ESFEMD-2): Compute $m_1 = F_s(x_1, x_2) = (s^2 - 1) \times x_1 + s^2 \times x_2 \bmod s^4$ for each block.

(ESFEMD-3): Convert m_1 into M .

Example 3.3. If the stego-image's pixels pair is $(y_1, y_2) = (163, 168)$ then we can get $m_1 = 13$ by using the extraction function $F_s(163, 168) = 15 \times 163 + 16 \times 168 \bmod 64 = 13$.

4. Simulation and Discussion. The proposed scheme was tested on ten 512×512 gray images (Lena, Baboon, F16, Barbara, Boat, Goldhill, Elaine, Tiffany, Pepper and Bridge) as shown in Fig.5. The corresponding stego images when $s = 2$ and $s = 3$ are shown in Fig.6 and Fig.7, respectively. There is no perceivable difference in appearance between cover images and stego images when $s = 2$. Although there are significant differences in visual between cover images and stego images when $s = 3$, the stegoimage quality is still acceptable. The experiment results are summed up in the table 1.

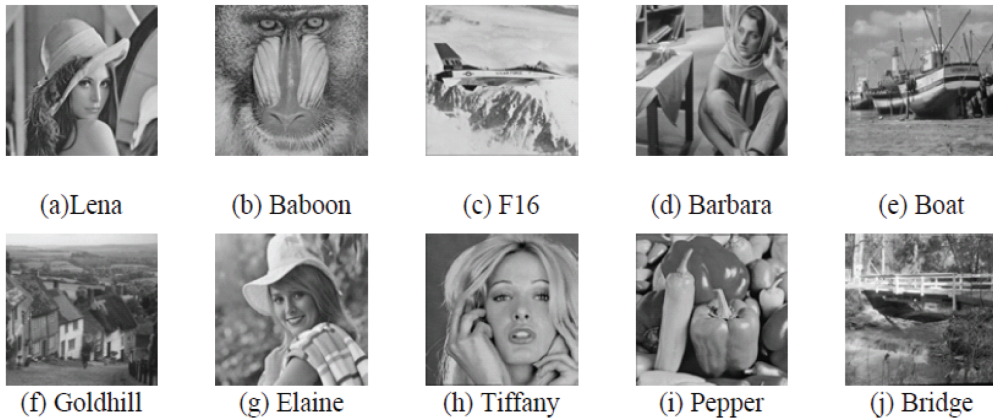


FIGURE 5. Ten 512×512 gray test images

Finally, we give some items, such as embedding function, embedding method, embedding capacity and storage space, to compare the difference between our scheme and the Kieu-Chang scheme[2] and then the results are shown as table 2.

Although our proposed scheme is similar to Kieu-Chang scheme, there are many advantages in our scheme which compared with the Kieu-Chang scheme. Firstly, in our model all embedding procedures are finished by using formula form. Secondly, the embedding rate is better than Kieu-Chang scheme in same modulus. Finally, our method does not require any memory space whereas Kieu-Chang scheme requires $\equiv 524$ Kbytes ($256 \times 256 \times 8 = 524.288\text{Kb}$) to store the embedding matrix.

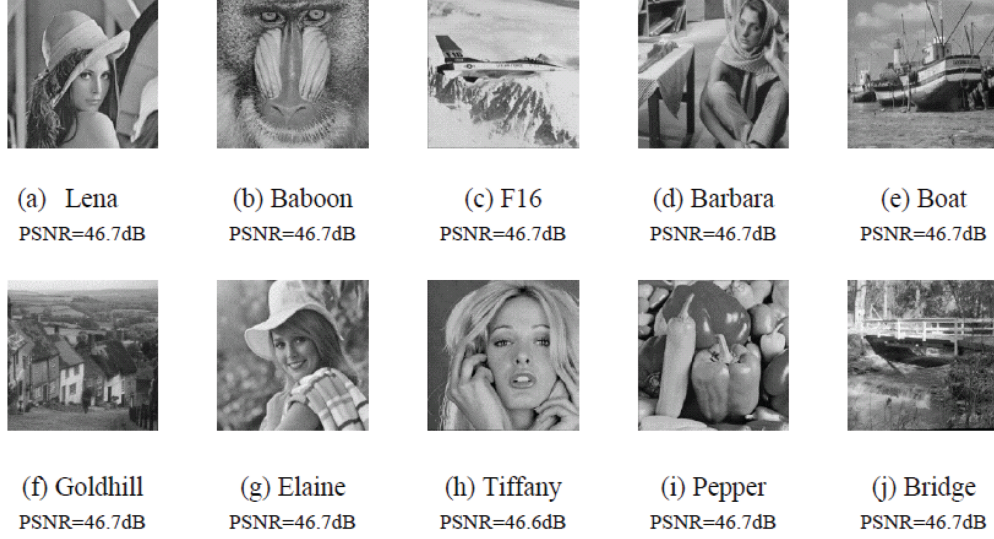


FIGURE 6. Ten 512×512 gray test images ($s = 2$)



FIGURE 7. Ten 512×512 gray test images ($s = 3$)

5. Conclusions. In order to enhance embedding capacity, a new data hiding scheme based on the SFEMD method is proposed in this paper. According to our simulation results, our proposed scheme can enhance the embedding rate and maintain the same embedding capacity but also keep good stego-image quality.

Acknowledgement: this work was supported by the National Science Council, R.O.C., under contract No.NSC-101-2221-E-224-100.

TABLE 1. Comparison table between Kieu-Chang method and our proposed scheme

Cover Image	Kieu-Chang method (s=4)	Our scheme (s=2)	Kieu-Chang method (s=9)	Our scheme (s=3)	Kieu-Chang method (s=16)	our scheme (s=4)
Lena	46.76	46.76	39.88	39.88	34.83	34.83
Bboon	46.75	46.75	39.90	39.90	34.83	34.83
F16	46.76	46.76	39.89	39.89	34.83	34.83
Barbara	46.75	46.75	39.89	39.89	34.84	34.84
Boat	46.76	46.76	39.89	39.89	34.82	34.82
Goldhill	46.76	46.76	39.90	39.90	34.83	34.83
Elaine	46.75	46.75	39.88	39.88	34.82	34.82
Tiffany	46.69	46.69	39.81	39.81	34.72	34.72
Pepper	46.75	46.75	39.89	39.89	34.83	34.83
Birdge	46.70	46.70	39.83	39.83	34.75	34.75

TABLE 2. Comparison characteristics between our scheme and Kieu-Chang scheme

Items	Kieu-Chang method	Our scheme
Embedding function	$[x_i \times (s - 1) + x_{i+1} \times s] \bmod s^2$	$[x_i \times (s^2 - 1) + x_{i+1} \times s^2] \bmod s^4$
Embedding method	S-Matrix	Mathematical method
Embedding Capacity when s=2	2 bpp	4 bpp
Storage space	524.288Kb	0

REFERENCES

- [1] A. Benhocine, L. Laouamer, L. Nana, and A. C. Pascu, New images watermarking scheme based on singular value decomposition, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 4, no. 1, pp. 9-18, 2013.
- [2] T. D. Kieu, and C. C. Chang, A steganographic scheme by fully exploiting modification directions, *Journal of Expert Systems with Applications*, vol. 38, no. 8, pp. 10648-10657, 2011.
- [3] W. C. Kuo, and C. C. Wang, Data hiding based on generalised exploiting modification direction method, *Journal of Imaging Science Journal*, available at <http://www.ingentaconnect.com/content/maney/isj/pre-prints/1743131X12Y.0000000011>, 2012.
- [4] W. C. Kuo, L. C. Wu, C. N. Shyi, and S. H. Kuo, A data hiding scheme with high embedding capacity based on general improving exploiting modification direction method, *Proc. of the Ninth International Conference on Hybrid Intelligent Systems*, pp. 69-72, 2009.
- [5] C. F. Lee, Y. R. Wang, and C. C. Chang, A steganographic method with high embedding capacity by improving exploiting modification direction, *Proc. of the Third International Conference on International Information Hiding and Multimedia Signal Processing*, pp. 497-500, 2007.
- [6] J. Mielikainen, LSB matching revisited, *IEEE Trans. Signal Processing Letters*, vol. 13, no. 5, pp. 285-287, 2006.
- [7] P. C. Ritchey, and V. J. Rego, A context sensitive tiling system for information hiding, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 3, no. 3, pp. 212-226, 2012.
- [8] R. Z. Wang, C. F. Lin, and J. C. Lin, Image hiding by optimal LSB substitution and genetic algorithm, *Journal of Pattern Recognition*, vol. 34, no. 3, pp. 671-683, 2001.

- [9] H. C. Wu, N. I. Wu, C. S. Tsai, and M. S. Hwang, Image steganographic scheme based on pixel-value differencing and LSB replacement methods, *IEE Proceedings. Vision, Image, and Signal Processing*, vol. 152, no. 5, pp. 611-615, 2005.
- [10] X. Zhang, and S. Wang, Efficient steganographic embedding by exploiting modification direction, *Journal of IEEE Communications Letters*, vol. 10, no. 11, pp. 781-783, 2006.